International Exchange Alumni (Alumni)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: International Exchange Alumni

(b) Bureau: Bureau of Educational and Cultural Affairs

(c) System acronym: IEA

(d) iMatrix Asset ID Number: 617

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): There are no changes since the last PIA assessment.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The current ATO has expired and we are currently going through the process of obtaining a new ATO. The next one is expected to be granted in July 2019.

(c) Describe the purpose of the system:
International Exchange Alumni is a dynamic and interactive networking website for past and current participants of U.S. government-sponsored exchange programs to build on their exchange experiences, network with fellow alumni, find grants and funding opportunities, and participate in alumni-only competitions.

By becoming a member of the Alumni site, exchange participants gain free access to these opportunities, plus a variety of paid journals and other online resources. They can also share news about their successful projects and celebrate the accomplishments of their fellow alumni around the world.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The system collects:

Birthday

Email address

First name

Last name

Gender

Home country

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

Mutual Educational and Cultural Exchange Act of 1961, 5 U.S.C. 301 2651a and 22 U.S.C. 3921

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: State-08 Educational and Cultural Exchange Program Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): August 10, 2007

☐No, explain how the information is retrieved without a personal identifier.

Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): N1-059-06-01, item 3
- Length of time the information is retained in the system: TEMPORARY: Destroy records no later than 75 years after birth date or earlier, if appropriate.
- Type of information retained in the system: Database of persons who have participated in a program fully or partially funded by the Bureau of Educational and Cultural Affairs (ECA) or predecessor organizations since 1970 for the purpose of coordinating or arranging alumni activities around the world. Records potentially include the following

information: name, gender, birth date, death date, citizenship, home and business addresses, and personal contact information about U.S. cities or states visited as part of a program.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No (SSNs not collected)

- If yes, under what authorization?

N/A

(c) How is the information collected?

User provides information directly on International Exchange Alumni website (https://alumni.state.gov).

(d) Where is the information housed?

☐ Department-owned equipment

☒ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

The site is hosted on IBM FEDRAMP-certified cloud environment through the hosting company SoftLayer.

(e) What process is used to determine if the information is accurate?

This information is verified by a system admin and is sometimes cross-referenced with the Alumni Archive. Other times, the information is verified with Program Officers of the exchange programs.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The information is correct and is verified by the owner of the information when they log into the website. The owner then has the opportunity to update their information via the website if it is incorrect.

(g) Does the system use information from commercial sources? Is the information publicly available?

This system does not use information from commercial sources or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes, a notice is provided to the individual prior to the collection of his or her information. The site has a Privacy Act Statement that details under what authority we can collect the information, the reason why we collect the information, how we will use the information and full disclosure.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

Individuals have to opt-in to providing their information for the Alumni site.

- If no, why are individuals not allowed to provide consent?

Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The site only collects the minimal information needed to confirm that individuals participated on a Department of State exchange program.

5. Use of information

(a) What is/are the intended use(s) for the information?

To confirm that individuals participated on a particular Department of State exchange program. The collected information may be used on a statistical basis to present information on activities of the U.S. State Department's international program participants to the U.S. Congress. The information is also used to connect alumni with other program participants.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, only individuals who have participated on a Department of State exchange program can have access to an account on the Alumni site.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
N/A

(2) Does the analysis result in new information?
N/A

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Information will be shared with other individuals who have accounts on the site if the user chooses to share that information and to the U.S. Congress.

(b) What information will be shared?
Home country, first/last name, and email address is shared.

(c) What is the purpose for sharing the information?
Information is shared so individuals can collaborate on projects with other users on the site.

(d) The information to be shared is transmitted or disclosed by what methods?
This information is shared via the user's profile on the site if that user chooses to share this information.

(e) What safeguards are in place for each internal or external sharing arrangement?
User must opt-in to sharing this information and only individuals who have been vetted can access this information. Individuals must have participated in a Department of State exchange program.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Since this is an externally hosted website with PII, it is vital that this information is protected. We only collect the minimum amount of information needed to confirm the individual participated in a Department of State exchange program and each individual is vetted before gaining access to the site.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
All collected PII is available on the individual's profile on the site. Individuals have access to their information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
Each individual has access to edit the information collected on their account by visiting their website profile. Users can edit their first name, last name, home country and email, but they cannot remove any of that information completely.

If no, explain why not.
N/A

(c) By what means are individuals notified of the procedures to correct their information?
An email is sent to individuals once their account has been approved with instructions on editing the information listed on their profile. There is also a Privacy Notice on the website that encourages individuals to edit and update their information and provides directions on how to access that information. The Privacy Act Statement can be found here: https://alumni.state.gov/about-international-exchange-alumni/terms-service/privacy-notice

8. Security Controls

(a) How is the information in the system secured?
Individuals must login to the secure site (per the hyperlink listed above) to access this information using a unique username and password. Also, this site is monitored by the hosting company system administrators 24 hours per day for suspicious activity.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.
Accounts must be approved by State Department officials or by developers on the site. The site used to manage access and view information is Drupal. Drupal roles act as layers, allowing users to have more than one role. A full matrix of Drupal roles and permissions can be accessed via https://alumni.state.gov/admin/people/permisions. Drupal has two basic role categorizations: **unauthenticated** and **authenticated** users. Unauthenticated users is the term Drupal uses for general website visitors who can see published public content. All other roles are categorized as authenticated and vary in role with regards to what kind of content and permissions users are able to view, once they are logged into the IEA website.

Once logged in, the following authenticated roles are able to perform the following functions:

Developer:

Top level access to site. Able to change settings and inherits all of the same permissions as the other roles listed below. The developer account is the highest level account and has access to all permissions and functionality that Drupal and its subsequent modules offer. Such items include -- but are not limited to -- changing website system info, adjusting user permissions, creating and adding new content types, editing existing content types and content, adding and removing users, and changing of user roles. Developer access is limited to only a handful of people from the Office of Public Affairs and Strategic Communications (PASC) in the Bureau of Educational and Cultural Affairs (ECA).

Administrator:

Access to view, edit and delete user accounts. Access to view, edit and delete web pages on site. The administrator role is the second highest level account with the ability to view/edit/delete user accounts and view/edit/delete web pages on the site. The administrator role is granted to PASC web producers and the web content manager to manage, update and publish content on web pages that is visible, when the page is published, to the general public and signed in alumni. The administrator can control which content is available to specific audiences: general public/unauthenticated users, authenticated U.S. exchange program alumni, and authenticated international exchange alumni.

Alumni Office Editor:

Access to view, edit, upload, verify, and delete user accounts. The Office of Alumni Affairs grants access by adding new exchange program alumni to its Alumni Archive. Only staff in the Office of Alumni Affairs has access. This role can view the following PII info: Date of birth, email address, full name (first, middle, last, second surname), nationality

DOS Personnel:

Access to view logged in portion of site DOS Personnel contact Office of Alumni Affairs and we verify user before granting this access level. Only DOS Personnel has the level of access. This role can only see their own PII information, which includes: Date of birth, email address, full name (first, middle, last, second surname), nationality

Alumni:

Access to edit own account, create projects and updates, and to view logged in portion of site

This is the default role for **any and all authenticated users** upon creating an account. The role allows individuals approved by the Alumni Office to create a user profile, where they are able to fill out personal information about what exchange programs they participated on, post updates, search for other users, and access alumni only exclusive content, such as research databases and funding opportunities.

Specific roles under Alumni access follow:

U.S. Exchange Alumni, Guest, U.S. Government, YALI Admin, YALI Washington Fellow, YALI Mentor, Embassy Contacts (YALI)

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The majority of information is accessible only to the system administrators. Only the user’s home country and email address is accessible to other users if the individual opts in to sharing that information. The system automatically tracks all users on the website and their browsing history is stored with the Drupal logs. The system stores 1,000,000 log messages, which can be audited/searched for system misuse. Server access is also tracked/logged and a notification email is sent to all Developers detailing all transactions performed by an individual who has logged in (or attempted to log in) to the system. . These logs are audited whenever there is a suspicion of misuse of the website's information.

(d) Explain the privacy training provided to authorized users of the system.
All system administrators are either DoS Federal Employees or DoS Contracted Employees, and must take PS800 - Cybersecurity Awareness, which has a privacy component, annually. All DoS Federal Employees are also required to take PA 459 – Protecting Personally Identifiable Information upon hire with the Department.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
The database that stores the data is encrypted using MD5 encryption and users must have an eight character alphanumeric password with Upper and Lower case characters.

(f) How were the security measures above influenced by the type of information collected?
The protection of PII is vital to the Department of State. Since the public accessible site that is managed through this system contains PII, it was essential to encrypt the database and to require a strong password for individual accounts, ensuring optimal safety precautions for the information stored.

9. Data Access

(a) Who has access to data in the system?
System Administrators and other authenticated users can access limited data, based on their access level. The data that each different role can access is listed in 8b of this document.

(b) How is access to data in the system determined?
Accounts must be approved by the site owner based on the assigned role to a user's account. One note about Drupal roles is that they act as layers, allowing users to have more than one role. A full matrix of Drupal roles and permissions can be accessed via https://alumni.state.gov/admin/people/permisions. Drupal has two basic role categorizations: **unauthenticated** and **authenticated** users. Unauthenticated users is the term Drupal uses for general website visitors who can see published public content. All other roles are categorized as authenticated and vary in role with regards to what kind of

content and permissions users are able to view, once they are logged into the IEA website. The Roles on the account include:

- Developer
- Administrator
- Alumni Office Editor
- DOS Personnel
- Alumni
- U.S. Alumni
- Guest
- U.S. Government
- YALI Admin
- YALI Washington Fellow
- YALI Mentor
- Embassy Contacts (YSEALI)

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access to all information is restricted to System Admins. Non System Admins only have access to the PII available to them based on their role. The PII available for each role is listed in 8b.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Access to this data is restricted to System Admins and other authenticated users who all have Secret clearances and are trusted to properly protect the information. The system automatically tracks all users on the website and their browsing history is stored with the Drupal logs. The system stores 1,000,000 log messages, which can be audited/searched for system misuse. Server access is also tracked/logged and a notification email is sent to all Developers detailing all transactions performed by an individual who has logged in (or attempted to log in) to the system.